

From: Getachew Tesfaye
Sent: Thursday, April 17, 2008 5:40 PM
To: Pederson Ronda M (AREVA NP INC)
Cc: John Smith; Terry Jackson; Michael Canova; Joseph Colaccino; William Kemper; Paul Loeser
Subject: Draft RAI 4 Software Program Manual Topical Report
Attachments: Draft RAI-4 ANP-10272 SPM TR.doc

Ronda,

Attached please find draft RAIs for ANP-10272, "Software Program Manual TELEPERM XS Tm Safety Systems Topical Report." We will have our technical Staff available to discuss them with you as soon as you are ready. Please call me with a proposed date and time for the telecon.

Please also review the RAI to ensure that we have not inadvertently included proprietary information. If there are any proprietary information, please let me know within the next ten days.

If I do not hear from you within the next ten days, I will assume there are none and will make the draft RAI publicly available.

Thanks,
Getachew Tesfaye
Sr. Project Manager
NRO/DNRL/NARP

INTERNET HEADERS:

Received: from HQCLSTR02.nrc.gov ([148.184.44.77]) by OWMS01.nrc.gov
([148.184.100.43]) with mapi; Thu, 17 Apr 2008 17:40:07 -0400
Content-Type: application/ms-tnef; name="winmail.dat"
Content-Transfer-Encoding: binary
From: Getachew Tesfaye <Getachew.Tesfaye@nrc.gov>
To: "Pederson Ronda M (AREVA NP INC)" <Ronda.Pederson@areva.com>
CC: John Smith <John.Smith@nrc.gov>, Terry Jackson <Terry.Jackson@nrc.gov>,
Michael Canova <Michael.Canova@nrc.gov>, Joseph Colaccino
<Joseph.Colaccino@nrc.gov>, William Kemper <William.Kemper@nrc.gov>, Paul
Loeser <Paul.Loeser@nrc.gov>
Date: Thu, 17 Apr 2008 17:40:04 -0400
Subject: Draft RAI 4 Software Program Manual Topical Report
Thread-Topic: Draft RAI 4 Software Program Manual Topical Report
Thread-Index: Acig05kFbllSKNJkT42eK/sYp6d/6A==
Message-ID: <C56E360E9D804F4B95BC673F886381E70A914A5C35@HQCLSTR02.nrc.gov>
Accept-Language: en-US
Content-Language: en-US
X-MS-Has-Attach: yes
X-MS-Exchange-Organization-SCL: -1
X-MS-TNEF-Correlator:
<C56E360E9D804F4B95BC673F886381E70A914A5C35@HQCLSTR02.nrc.gov>
MIME-Version: 1.0

DRAFT

FOURTH REQUEST FOR ADDITIONAL INFORMATION (RAI)

ANP-10272, "SOFTWARE PROGRAM MANUAL FOR TELEPERM XS™ SAFETY SYSTEMS TOPICAL REPORT"

**TAC NO. MD3971
DOCKET NO. 52-052**

**Discipline: Digital I&C
Organization: NRO/DE/ICE2**

RAI-71.

Question:

What is AREVA NP's justification for deviating from IEEE 1012-1998 in allowing the software design organization to design and run verification and validation (V&V) tests in place of the V&V organization?

Concern:

The V&V organization exists as a separate check and balance to the design engineering and software organizations to provide a high degree of confidence in the compliance with functional, performance, and interface requirements; and in the completeness and correctness of the software or system in question. The V&V team, in some ways, may be viewed as a layer of diversity and defense-in-depth in the quality, design, and testing processes.

IEEE 1012 makes the generation and execution of various test plans the duty of the V&V organization.

Allowing the software design organization to design and run V&V tests in place of the V&V organization indicates a loss of that diverse defensive layer in a safety-critical stage of software testing. Various errors of interpretation and implementation which may have been introduced into the software by the thinking of the software design organization will likely be masked in the design and execution of the V&V tests through those same pathways of interpretation if executed by the same organization. AREVA NP has not explained or justified how its procedures and methods will mitigate these possible errors in lieu of fully complying with IEEE 1012 (by maintaining the V&V organization's complete responsibility for the design and execution of V&V tests). It has also not detailed any specific requirements of the V&V organization in this scenario.

It should be noted, however, that while the responsibility of generating V&V test plans and procedures lies solely with the V&V organization, the design engineering personnel may carry out the actual tests.

AREVA NP has also proposed that there may be precedence in the Common Q Safety Evaluation Report (SER) for allowing this exception. It should be understood, however, that the Common Q topical Safety Evaluation (SE) exception does not justify AREVA NP's proposal in that it differed from AREVA NP's methods in at least two significant ways:

1. The Common Q topical included detailed procedures and responsibilities for the V&V organization to execute in the case that another organization designs and runs a V&V test. AREVA NP's Software Program Manual (SPM) does not contain any additional information beyond the statement of deviation.
2. The Common Q topical exception was taken in context of the overall Common Q quality assurance and V&V methods, which in general, go into greater detail than the AREVA NP SPM.

The staff requires additional information to determine if the proposed alternative to the requirements of IEEE 1012 will provide an equivalent confidence in a high quality test process, and therefore an equivalent confidence in the safety of the resultant system.

AREVA NP's response should include the following:

- Documentation of independent V&V Group's Assessment of Testing
- Documentation of V&V Group's Role/Interaction with design and the Test Group
- Documentation of how Problems identified by the test are resolved and the V&V Group's role in that process
- Clear delineation of responsibility and authority of the V&V team over the V&V testing, planning, design, execution, and review

Applicant Reference(s):

ANP-1072

Simulation Testing (Page 6-7)

As a minimum, the verification and validation engineer reviews the simulation test plan and results of the testing to ensure that the requirements are adequately tested.

1. *In the event that SIVAT testing is only performed by design engineering with a complete factory acceptance test, **the verification and validation team only performs the reviews.***

RAI-72.

Question:

Where the AREVA NP SPM states that it conforms, complies, or uses similar language with regard to a particular industry standard, NRC regulation, or NRC guidance, is the SPM in fact stating 100% compliance to that reference (except, of course, where specific exceptions are identified and described in the SPM)? This is a “yes” or “no” question. If the answer is “no,” identify deviations from the standards, regulations, and guidance used in the SPM.

Concern:

Within the text of the SPM, there are multiple instances of conformance claims. The majority of the conformance claims use similar language to describe conformance. Some sections of the SPM describe deviations from conformance where previous text in the same section seemed to describe full conformance. Other sections of the SPM state “applicable” conformance, but do not go on to list what is not applicable nor give explanation for that claim. This intermittent identification of deviations from standards, guidance, and regulations seems to indicate that AREVA NP only generally follows those documents in executing the SPM, and gives no guarantee that all intended exceptions have been identified in the SPM.

Unless AREVA NP specifically states and lists exceptions in the SPM, the NRC must consider that the SPM dictates full compliance with referenced standards, guidance, and regulations. The associated SE for the SPM will be written to reflect that understanding, and any combined license application (COLA), license amendment request (LAR), or design certification (DC) referencing the SPM will be held to the same scrutiny of full compliance unless those documents take specific exception. Furthermore, in the case of a review where it is found that an application referencing the AREVA NP SPM has deviated from the SPM, in the aforementioned understanding, and without stating explicit exceptions, that application will have to be considered in non-compliance with the AREVA SPM.

Where the SPM states that it takes exception to compliance, or only applies to applicable sections, without listing and explaining those exceptions or applicability, AREVA should revise the SPM’s language and add amplifying information.

Applicant Reference(s):

The following is a list of examples, though it is not exhaustive:

ANP-1072

Test Planning (Page 3-5)

*Testing activities **follow** the guidance of IEEE 829 (Reference 19), which is endorsed by Regulatory Guide 1.170 (reference 7)...*

Methodology for Generating the Software Requirements Specification (Page 3-7)

*The software design group **follows** the guidance in IEEE 830 (Reference 20), which is endorsed by Regulatory Guide 1.172 (Reference 9), **as the preferred method** for the creation of the SRS...*

Software Safety Plan (Page 4-1)

The plan follows the concepts of IEEE 1228 but does not fully comply (Reference 28).....

Software Verification and Validation Plan (Page 6-1)

*The Software Verification and Validation Plan follows the guidance of the **applicable** recommendations of IEEE 1012, which is endorsed by Regulatory Guide 1.168. **One area of exception** with regard to the IEEE Standard 1012 is...*

Test Plan (Page 9-4)

*Software simulation testing with SIVAT is planned and executed in accordance with procedures **following** the **applicable** recommendations of IEEE 1008 (Reference 21), which is endorsed by Regulatory Guide 1.171 (reference 8).*

RAI-73.

Question:

What is AREVA NP's justification for crediting SIVAT testing in reducing the scope of the factory acceptance test (FAT) and other unit and integration testing?

Concern:

AREVA NP's SPM, in combination with the TELEPERM XS topical report, does not contain enough information for the NRC to make a determination as to the acceptability or safety of the software testing process in terms of the coverage of the testing or with regard to the tools used to accomplish that testing.

Specifically, the following information is lacking:

1. The scope and coverage of SIVAT and FAT testing, in combination and separately
2. The capabilities, qualification, and implementation of SIVAT
3. Information on integration and unit testing; and how that testing may be satisfied by a combination of SIVAT and FAT testing
4. Details of the SIVAT and FAT tests
5. Justification for reducing the FAT tests
6. Guidelines for determining the extent to which FAT coverage may be reduced by SIVAT testing

In general, there is no way for the NRC to understand what is meant by a reduction in FAT testing with the information currently provided by AREVA NP. It appears that SIVAT simulates the software's operation. With the use of SIVAT, AREVA NP needs to demonstrate how FAT will fully verify and validate software/hardware integration aspects. AREVA NP should provide procedures and processes that will ensure software/hardware integration aspects are appropriately addressed in the proposed V&V scheme.

It should also be understood that SIVAT is not an approved tool. While the concept of simulated testing was mentioned briefly in the TELEPERM XS topical report, the SIVAT tool was not described, nor was it approved by the associated SER. As such is the case, a reference to the TELEPERM XS topical or SER is not considered sufficient justification or explanation for the SIVAT, FAT, unit, and integration testing proposed by the SPM.

The SPM relies heavily on the concept of SIVAT as a tool, in combination with FAT, for V&V in place of more traditional methods. As such is the case, the approval of the SPM may be predicated upon NRC's understanding and acceptance of the SIVAT tool and AREVA NP's FAT methodologies and procedures.

AREVA NP Report No. NGLP/2004/en/0094, "TELEPERM XS Simulation - Concept of Validation and Verification" should be submitted to support AREVA NP's explanation of SIVAT.

Applicant Reference:

Simulation Testing (Pages 6-7,8)

*If the verification and validation team performs tracing or SIVAT testing and tracing, **the testing can be credited to reduce the scope of the factory acceptance test.** Three options can be used to determine the verification and validation scope:*

- 1. In the event that SIVAT testing is only performed by design engineering with a complete factory acceptance test, the verification and validation team only performs the reviews.*
- 2. The verification and validation team can trace the requirements through the SIVAT testing as performed by design engineering, **in which case the scope of the factory acceptance testing will be reduced.***
- 3. The verification and validation team can plan and perform SIVAT testing in addition to tracing, in which case the factory acceptance test scope will be reduced.*

RAI-74.

Question:

How does the use of SIVAT:

Ensure a high-quality test process and safety of the resultant system which is equivalent or better than traditional unit and integration testing.

and

Demonstrate that the system requirements specifications have been correctly translated into error-free application code?

Concern:

The SPM indicates that the SIVAT tool (Simulation and Validation Tool) makes unit and integration tests unnecessary. This approach is unfamiliar to the staff and does not appear to be consistent with industry standards and regulatory guidance.

The use of the SIVAT tool was not identified in the TXS topical report, and it is not clear if the software tested by SIVAT is the same compiled application code to be loaded, unaltered, onto TELEPERM XS hardware. It appears that the first time the compiled operational code is tested is during the FAT, which is developed by the design and test group, not the V&V Group.

The staff does not understand, based on the limited information submitted describing SIVAT and the V&V process, how software testing using SIVAT can demonstrate that the system requirements specifications have been correctly translated into error-free application code. The staff believes that testing performed by unit and integration tests should be performed on the actual operational code, and therefore it may be necessary to perform additional software testing.

In addition, it should be understood that test plans and procedures generation and verification are the sole responsibility of the V&V team. The existence of an automated tool does not relieve the V&V team of their responsibilities.

AREVA NP's response should support a conclusion that the SIVAT testing will provide confidence in a high quality test process and equivalent confidence in the safety of the resultant system.

AREVA NP Report No. NGLP/2004/en/0094, "TELEPERM XS Simulation - Concept of Validation and Verification" should be submitted to support AREVA NP's explanation of SIVAT.

Demonstration of the SIVAT tool and associated development and V&V tools may contribute to the NRC staff's confidence and understanding of AREVA NP's

approach as outlined in the SPM. Arrangement of such a demonstration may be coordinated through the NRC's EPR Projects Branch.

Applicant Reference:

ANP-1072

Software Safety Plan (Page 4-1)

... AREVA NP uses SIVAT testing of the application software generated by the SPACE tool to detect errors that would prevent the software from fulfilling its safety function. SIVAT testing, coupled with the FMEA, response time analysis, and FAT are sufficient to ensure that there are no software hazards...

RAI-75.

Question:

Has the SIVAT tool been qualified in a manner similar to that required for software performing safety-related functions, and does the software lifecycle process of the SIVAT tool development meet the requirements for that type of software?

Concern:

The SPM describes the SIVAT tool as a key component in the application software V&V testing. Since the safety and quality of the resultant application software is paramount, tools used to assure that quality and safety should be, in of themselves, high quality. No such demonstration of quality has been made for the SIVAT tool.

The TELEPERM XS and SPM topical reports lack details about the qualification of the SIVAT software and the process quality used in the SIVAT tool development.

AREVA is requested to submit additional information to support any qualification claims for the SIVAT tool.

Applicant Reference:

ANP-1072

RAI-76.

Question:

According to the SPM, is the QA Manager responsible for determining if the QA procedures are adequate?

If not, to what extent is that responsibility transferred, and what is the justification for giving the Technical Manager this responsibility?

Concern:

The language of the SPM seems to indicate that the Technical Manager is assuming the responsibilities of the Quality Assurance (QA) Manager. If this is the case, then AREVA NP would have to indicate the extent to which the QA Manager responsibilities have been transferred to the Technical Manager and justify how this maintains a high-quality process. The NRC would then determine the acceptability of such a justification.

However, if the intent of the language in the SPM is to indicate that the Technical Manager is responsible for ensuring that his group follows the QA plans, while the QA Manager retains responsibility for managing and ensuring the adequacy of processes and procedures in those plans, the language of the SPM should be refined to more clearly indicate this standard approach. Submit any page changes needed for this clarification.

Applicant Reference:

ANP-1072

Technical Manager (Page 2-2)

*Under the implementing procedures of the AREVA NP Quality Management Manual, the **technical manager is responsible for ensuring that the applicable QA processes and procedures are implemented on all projects.***

Management (Page 3-1)

The technical manager manages the Software Quality Assurance Plan. The QA group verifies that the implementation of QA requirements is in accordance with the Quality Management Manual. The technical manager ensures that software and associated documentation has been developed in accordance with the Software Quality Assurance Plan, which includes ensuring that the testing and documentation requirements established in the test plan have been followed.

RAI-77.

Question:

According to the SPM, is the V&V Manager responsible for the disposition of discrepancy reports by ensuring that the actions taken and changes made in such disposition are correct, appropriate, and sufficient?

If not, what is the justification for giving the Technical Manager this responsibility?

Concern:

The language of the SPM seems to indicate that the Technical Manager is assuming the responsibilities of the V&V Manager. If this is the case, then AREVA NP would have to indicate the extent to which the V&V Manager responsibilities have been transferred to the Technical Manager and justify how this maintains a high-quality, verified and validated process. The NRC would then determine the acceptability of such a justification, though it is likely that such a deviation from standard V&V practices would be found unacceptable.

If the SPM indicates the V&V Manager is, in fact, responsible for such disposition, the SPM language should be refined to clearly indicate this standard approach. Submit any page changes needed for this clarification.

Applicant Reference:

ANP-1072

Technical Manager (Page 2-2)

The technical manager is responsible for disposition of discrepancy reports and other anomalies generated in the course of verification and validation.

RAI-78.

Question:

What is AREVA NP's justification in reducing the scope of the software integration effort?

In answering this question, please also address:

What is the specific reduction in scope of integration efforts?

What functionality of the SPACE tool, or effort occurring during the SPACE tool development, is considered to alleviate the need for separate software integration testing?

Concern:

AREVA NP has not provided enough information explaining what is considered to be the reduced scope of integration testing.

AREVA NP has not provided justification for reducing the scope or entirely eliminating software integration testing.

AREVA NP has not proposed a sufficient explanation as to why the SPACE tool surpasses integration testing. Neither has the functionality of the SPACE tool been described to an extent that builds the case for its use instead of integration testing.

Submit the appropriate page changes in the SPM to support the justification.

Applicant Reference:

ANP-1072

I&C Engineers (Page 2-4)

*Because the application software is generated by the SPACE tool and the SPACE tool is designed to provide the software to run on the TELEPERM XS system software, **no separate integration effort for this software is required.***

RAI-79.

Question:

Does the V&V team

Ensure that the outputs of each phase of the design process fulfill the requirements of each previous phase,

and

Determine that the design outputs comply with functional, performance, and interface requirements through tests and inspections?

Concern:

The language of the SPM seems to indicate that the responsibility of the V&V team is limited to the traceability analysis and the functional requirements specification (FRS) review. The SPM does not indicate that the V&V team will fulfill the V&V team responsibilities as described by relevant IEEE standards.

IEEE 100 defines the following:

verification: The process of determining whether or not the product of each phase of the digital computer system development process fulfills all the requirements imposed by the previous phase.

validation: The test and evaluation of the integrated computer system to ensure compliance with the functional, performance, and interface requirements.

verification and validation: The process of determining whether the requirements for a system or component are complete and correct, the products of each development phase fulfill the requirements or conditions imposed by the previous phase, and the final system or component complies with specified requirements.

Any deviation from these definitions in the responsibilities or methods of the V&V team should be identified and justification should be provided for those deviations, including necessary page changes to the SPM.

Applicant Reference:

ANP-1072

Verification and Validation Team (Page 2-5)

The verification and validation team performs verification reviews of the FRS and the traceability analysis of the SRS into design and test plans.

RAI-80.

Question:

Does AREVA NP understand that where the SPM references other material in support of fulfilling requirements, that material must be subject to review and inspection by the NRC in making any determination of conformance, safety, and acceptability for any given application, design certification, or amendment?

Concern:

The SPM sets forth requirements and objectives for various software lifecycle and other plans, and in many places it references other documents to make claims of full conformance to guidance, regulations, and standards. While the sum of these pieces may ultimately be found acceptable for a specific application, it cannot be assumed that the approval of one high-level document (SPM) cascades to its subordinate and referenced documents. Every document referenced in support of the SPM and the plans it describes must be considered on its own merit.

One such example is the reference of the AREVA NP Quality Management Manual. AREVA NP indicates that the Software Quality Assurance Plan does not fulfill IEEE 730 requirements on its own, but in combination with the AREVA NP Quality Management Manual and QA reviews and audits. AREVA NP does not delineate which portions of IEEE 730 are covered by the SQAP and which portions are covered by the Quality Management Manual, nor does AREVA NP provide the Quality Management Manual for review. For any license amendment request, combined license application, or design certification referencing the SPM in support of the SQAP, the NRC will have to review, inspect, or audit; and find acceptable; the Quality Management Manual and associated operating instructions. This example extends to all of the plans described by SPM.

Applicant Reference:

ANP-1072

Introduction (Page 1-1, 2)

In addition to this Software Program Manual, the program consists of the following plans:

- 1. Software Quality Assurance Plan, which describes the necessary processes that ensure that the software attains a level of quality commensurate with its importance to safety function.*
- 2. Software Safety Plan, which identifies the process to reasonably eliminate hazards that could jeopardize the health and safety of the public from safety critical software.*

3. *Software Verification and Validation Plan, which describes the method that ensures correctness of the software.*
4. *Software Configuration Management Plan, which describes the method that maintains the software in a controlled configuration at all times.*
5. *Software Operations and Maintenance Plan, which describes post-customer delivery software practices.*

The combination of the Software Program Manual and the five plans above constitute a program that conforms to the guidance of Nuclear Regulatory Commission (NRC) Branch Technical Position (BTP) Human, Instrumentation and Controls Branch Topical (HICB)-14 (Reference 11)...

*...The Software Program Manual establishes the requirements and objectives for the Software Quality Assurance Plan, Software Safety Plan, Software Verification and Validation Plan, Software Configuration Management Plan, and Software Operations and Maintenance Plan. These five plans are implemented as AREVA NP operating instructions and will conform to the requirements established in the Software Program Manual. **In some cases additional operating instructions will be used to define specific implementation details. For example, the Software Configuration Management Plan is defined in an operating instruction and additional administrative controls for the software library are specified in a separate operating instruction.** Operating instructions established for these five plans are available onsite at AREVA NP facilities to support NRC review of this topical report.*

Purpose (Page 3-1)

*The Software Quality Assurance Plan fulfills the requirements for a software quality assurance plan in accordance with IEEE 730 (Reference 17) **but must be considered along with the AREVA NP Quality Management Manual and the Quality Assurance reviews and audits for complete fulfillment of the IEEE requirements.***

RAI-81.

Question:

What is the extent of the project manager's assessment of software safety risk in accordance with IEEE 7-4.3.2?

Concern:

The language in the SPM indicates that the project manager assesses technical, schedule, and regulatory risks of software projects. It is unclear what the SPM means by "technical" risks, as it is not defined nor is it a common term used in IEEE 7-4.3.2. Schedule and regulatory risks, while of concern to an operating business, are not of interest to the NRC in making safety determinations. This section of the SPM does not emphasize the safety risk of the project.

A project manager's assessment of software safety risk should take into account product engineering, development environment and program constraints, system risks, mechanical/electrical hardware integration, risks due to size and complexity of the product, the use of pre-developed software, risks from program interfaces, maintenance risk, security risk, and the risk associated with each V&V task; and should follow the requirements of IEEE 7-4.3.2.

IEEE 7-4.3.2 contains a section on software project risk management (5.3.6) which defines a concept and outlines the appropriate steps to take in analyzing and implementing risk management. If this is what AREVA NP intends by use of the term "technical" risk, the language of the SPM should be clarified to represent this intent.

If AREVA NP intends a different interpretation, a justification for deviating from IEEE 7-4.3.2 should be made. Submit any page changes necessary for that justification.

An excerpt from IEEE 7-4.3.2, Section 5.3.6 follows:

Software project risk management is a tool for problem prevention: identifying potential problems, assessing their impact, and determining which potential problems must be addressed to assure that software quality goals are achieved. Risk management shall be performed at all levels of the digital system project to provide adequate coverage for each potential problem area. Software project risks may include technical, schedule, or resource-related risks that could compromise software quality goals, and thereby affect the ability of the safety computer system to perform safety related functions. Software project risk management differs from hazard analysis, as defined in 3.1.31, in that hazard analysis is focused solely on the technical aspects of system failure mechanisms.

Risk management shall include the following steps:

- a) Determine the scope of risk management to be performed for the digital system.*
- b) Define and implement appropriate risk management strategies.*

- c) *Identify risks to the software project in the project risk management strategy and as they develop during the conduct of the project.*
- d) *Analyze risks to determine the priority for their mitigation.*
- e) *Develop risk mitigation plans for risks that have the potential to significantly impact software quality goals, with appropriate metrics for tracking resolution progress. (These risks may include technical, schedule, or resource-related project risks that could compromise the ability of the safety computer system to perform safety related functions.)*
- f) *Take corrective actions when expected quality is not achieved.*
- g) *Establish a project environment that supports effective communications between individuals and groups for the resolution of software project risks.*

Applicant Reference:

ANP-1072

Risk Management (Page 3-10)

The project manager identifies and assesses the technical, schedule, and regulatory risks of the project.

RAI-82.

Question:

Is the Diversity and Defense-in-Depth analysis the only place where a software common mode failure is considered?

Concern:

The SPM states that "...the FMEA does not need to consider the effects of a software common-mode failure because this kind of failure is handled by the diversity and defense-in-depth analysis..." This statement is incorrect. Position 3 of the SRM to SECY 93-087 specifically requires that the licensee consider a postulated common-mode failure. Furthermore, the purpose of the D3 analysis, in part, is to support the findings in the FMEA.

If the intent of the SPM is, however, that software common mode failure is considered elsewhere, the language of the SPM should be revised to clearly reflect where it is considered. Submit any page changes necessary to reflect this clarification.

One example of such a clarification could be:

"However, the FMEA does not need to consider the effects of a software common mode failure because this kind of failure is considered in ... to assure that the plant specific diversity and defense-in-depth will handle the postulated software common mode failure."

Applicant Reference:

ANP-1072

Failure Modes and Effects Analysis (Page 4-3)

However, the FMEA does not need to consider the effects of a software common mode failure because this kind of failure is handled by the diversity and defense-in-depth analysis discussed in Section 4.3.1.

RAI-83.

Question:

Does the SPM indicate by stating that a software safety organization is not necessary that a software hazard analysis is also not necessary? If so, what justification, beyond what is already provided in the SPM, does AREVA NP propose for the elimination of the software hazard analysis? If AREVA NP does intend to perform a software hazard analysis, what language indicates this in the SPM?

Concern:

The SPM language seems to indicate that test, FMEA, response time analysis, and FAT are sufficient to eliminate the need for a software hazards analysis. If this were the case, any system with adequate test, analysis, and V&V would be exempt from the need for the software hazards analysis. This, however, is not the case.

The software hazards analysis is used to look at failures such as software malfunctions which could defeat the safety function, failures induced by use of out-dated procedures, system I/O incompatibilities (electrical/mechanical) with plant interfaces, and failures with hard to notice or no indications, and so on.

Often, a software hazards analysis is not a separate analysis, but part of a larger safety analysis or some other analysis which specifically looks for software hazards. If AREVA NP has included the software hazards analysis as part of some other analysis, the SPM language should be revised to clarify that inclusion and state where the software hazard analysis occurs.

If, however, AREVA NP intends to deviate from having a standard software hazard analysis due to the use of SIVAT as a V&V tool, the quality and capability of the SIVAT tool would have to be demonstrated and the NRC would have to find it of a quality suitable for use in safety-related applications to consider this alternative.

Applicant Reference:

ANP-1072

Software Test Report on SIVAT Testing (Page 4-4)

The SIVAT tool tests the functionality of the software and provides the results. The verification and validation organization reviews the results of the simulation testing. This approach is different than the guidance of BTP HICB-14. AREVA NP concluded that an independent software safety organization is not necessary to perform this testing. Independent reviews of the work done with SPACE and SIVAT performed by the verification and validation organization, coupled with the FMEA, response time analysis, and FAT are sufficient to ensure that there are no software hazards.

RAI-84.

Question:

What is AREVA NP's justification for not using a software configuration management organization or software configuration control board for software configuration management?

Concern:

There is no justification given for not having a configuration control board. This type of board is specifically relied upon to ensure that all configuration changes are adequately and appropriately justified, tested, and documented, and that the urgencies of the project cost and schedule do not permit changes to be made without this justification, test, and documentation.

Applicant Reference:

Organization (Page 5-2)

The software engineering group performs the software configuration management activities described in this Software Configuration Management Plan. The software supervisor is responsible for these activities. As such, no separate software configuration management organization is required for the implementation of the software configuration management activities on a TELEPERM XS software project. The organization is as described in Section 2.0 above."

Configuration Control Boards (Page 5-4)

AREVA NP does not use configuration control boards for software configuration management.

RAI-85.

Question:

What is AREVA NP's justification for taking exception to IEEE 1012 in reducing the scope of component V&V? How does AREVA NP determine what will undergo component V&V and what will not?

Concern:

AREVA NP proposes an exception to IEEE 1012 that has not been adequately justified. Furthermore, the differentiation of what is to undergo component V&V and what is not has not been described—no methodology for making that determination has been proposed.

The NRC cannot make a determination as to the acceptability of this deviation or exception based on the limited information provided by AREVA NP. AREVA NP will have to provide additional information to assure that the deviation from IEEE 1012 will support an equivalent level of resultant software safety or indicate full conformance with IEEE 1012.

Applicant Reference:

Software Verification and Validation Plan (Page 6-1)

*The Software Verification and Validation Plan follows the guidance of the applicable recommendations of IEEE 1012, which is endorsed by Regulatory Guide 1.168. **One area of exception** with regard to the IEEE Standard 1012 is that **component verification and validation test execution is not considered to be mandatory**, but verification of any component testing performed is mandatory.*

RAI-86.

Question:

In determining that the Software Verification and Validation Plan is appropriate to the scale and complexity of the project, does the design technical manager serve as a consultant to the QA manager, or does the design technical manager have authority in that determination?

Concern:

The QA and V&V organizations are the only organizations with any authority over the Verification and Validation Plan. The design technical manager is not independent, and could be influenced by non-quality factors such as cost or scheduling issues. The V&V and QA organizations can, however, request the consultation of other organizations and managers, such as the design technical manager, in collecting information from which to base their determination. If this is the intent of the SPM language, it should be modified to clearly state that relationship. The current language of the SPM in this regard is inappropriate.

This raises similar concerns as expressed in RAI #76.

Applicant Reference:

Organization (Page 6-2)

The design technical manager and the QA organization are responsible for determining that the Software Verification and Validation Plan is appropriate to the scale and complexity of the project.

RAI-87.

Question:

How does a commonly understood notation facilitate verification of function diagrams? What, precisely, is meant by “a commonly understood notation?”

Concern:

The SPM does not explain what notation is used to facilitate verification of function diagrams, why that notation is considered to be commonly understood, or how the use of common notation facilitates the verification process.

While using a commonly understood notation is generally good practice, AREVA NP needs to further explain this statement in the SPM. The commonly understood notation methodology used by AREVA NP should be explicitly stated, as the argument will be self-evident if the identified notation is commonly recognized. If, however, the notation is specialized but commonly understood among AREVA NP employees, for example, the statement should be qualified in such a manner.

Applicant Reference:

Simulation Testing (Page 6-8)

4. *The verification of the function diagrams by the engineers is facilitated by the use of a commonly understood notation.*